UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/733,537	12/07/2000	Philip R. Graham	CSCO-86861	1789

7590 11/16/2005

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/733,537	GRAHAM, PHILIP R.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 are pending in this office action, claims 1, 7, and 17 are amended.

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this office action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

3. Claims 1, 2, 4, 5, 7-12, and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6,389,532) in view of Boyle et al. (U.S. Patent No. 6,212,636), and further in view of Bruck et al. (U.S. Patent No. 6,691,165).

Regarding claim 1, Gupta et al. teaches a digital signature method for a network infrastructure copy protection system (fig. 1), comprising:

- Applying a digital signature to a digital content file (col. 3, line 41-48);
- Transmitting the content file across a distributed computer network (col. 3, lines 49 and 50);
- Examining the content file to determine whether the content file includes the digital signature, the examining performed within the distributed computer network (col. 3, lines 50-54);

- Transmitting the content file when the content file includes the digital signature (col. 4, lines 7-11);
- Blocking transmission of the content file when the content file does not include the digital signature (col. 4, lines 12 and 13).

Gupta et al. does not teach blocking transmission of the content file when the data comprising the content file is a restricted data format.

Boyle et al. teaches blocking transmission of the content file when the data comprising the content file is a restricted data format (col. 1, lines 36-40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine blocking transmission of the content file when the data comprising the content file is a restricted data format, as taught by Boyle et al., to the digital signature method of Gupta et al. It would have been obvious for such modifications because blocking restricted data formats prevent network congestion. By only allowing text and other small data files to transmit, the burden of transmitting video or audio is eliminated. This is especially important when the receiving device can't handle the restricted data type (see col. 1, lines 38-40 of Boyle et al.).

The combination of Gupta et al. in view of Boyle et al. does not teach the embodiment to be in **a load balancer**, but rather a router. However, Bruck et al. teaches that a router can be a load balancer (col. 1, lines 55-59).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a load balancer for blocking, as taught by Bruck et al., to the digital signature method of Gupta et al/Boyle et al. It would have been obvious for such modifications because load balancing distributes the load evenly over several network devices so that any one device will not experience an overwhelming amount of traffic. To modify the router of Gupta et al./Boyle et al. with the Bruck et al. reference that explains routers can be load balancers, provides motivation for the combination.

Regarding claim 7, Gupta et al. teaches a restricted data format method for a network infrastructure copy protection system, comprising:

- Receiving a digital content file for transmission across a distributed computer network (fig. 7, ref. num 702);
- Examining data comprising the content file, the examining performed within the distributed computer network (fig. 7, ref. num 704 and 706).

Gupta et al. does not teach examining data comprising the content file to determine whether the content file includes a restricted data format. Gupta et al. also

does not teach transmitting the data file if the data comprising content file does not include the restricted data format, and blocking the file if the data comprising content file does include the restricted data format.

Boyle et al. teaches examining data comprising the content file to determine whether the content file includes a restricted data format, transmitting the data file if data comprising the content file does not include the restricted data format, and blocking the file if data comprising the content file does include the restricted data format (col. 1, lines 36-40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine examining data comprising the content file to determine whether the content file includes a restricted data format, transmitting the data file if data comprising the content file does not include the restricted data format, and blocking the file if data comprising the content filed does include the restricted data format, as taught by Boyle et al., to the restricted data format method of Gupta et al. It would have been obvious for such modifications because examining the content file and transmitting based on the lack of the restricted data format or blocking based on the presence of the restricted data format prevents network congestion. By only allowing text and other small data files to transmit, the burden of transmitting video or audio is eliminated. This is especially important when the receiving device can't handle the restricted data type (see col. 1, lines 38-40 of Boyle et al.).

The combination of Gupta et al. in view of Boyle et al. does not teach the embodiment to be in **a load balancer**, but rather a router. However, Bruck et al. teaches that a router can be a load balancer (col. 1, lines 55-59).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a load balancer for blocking, as taught by Bruck et al., to the restricted data format of Gupta et al/Boyle et al. It would have been obvious for such modifications load balancing distributes the load evenly over several network devices so that any one device will not experience an overwhelming amount of traffic. To modify the router of Gupta et al./Boyle et al. with the Bruck et al. reference that explains routers can be load balancers, provides motivation for the combination.

Regarding claim 2, the combination of Gupta et al. in view of Boyle et al./Bruck et al. teaches the digital signature is configured to identify the sender of the digital content file (see col. 3, lines 44-46 of Gupta et al.).

Regarding claims 4 and 11, the combination of Gupta et al. in view of Boyle et al./Bruck et al. teaches the distributed computer network is the Internet (see col. 5, lines 15-20 of Gupta et al.).

Regarding claims 5 and 12, the combination of Gupta et al. in view of Boyle et al./Bruck et al. teaches the examining is performed by a plurality of routers within the distributed computer network (see fig. 1, ref. num 104 of Gupta et al.).

Regarding claims 8-10, and 14-16, the combination of Gupta et al. in view of Boyle et al./Bruck et al. teaches the restricted data format is an MP3 data format, a MPEG video data format, and a Word document format (see col. 1, lines 36-40 of Boyle et al.).

Claims 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (USPN '532) in view of Boyle et al. (USPN '636), and further in view of Gibbs et al. (U.S. Patent No. 6,085,321).

Regarding claim 17, Gupta et al. teaches a network infrastructure protection method for detecting and denying transmission of restricted data formats, comprising:

- Receiving a digital content file for transmission across a distributed computer network (fig. 7, ref. num 702);
- Examining data comprising the content file, the examining performed within the distributed computer network (fig. 7, ref. num 704 and 706).

Gupta et al. does not teach examining data comprising the content file to determine whether the content file includes a restricted data format, wherein the content

file is free of a digital signature. Gupta et al. also does not teach transmitting the data file if the data comprising content file does not include the restricted data format, and blocking the file if the data comprising content file does include the restricted data format.

Boyle et al. teaches examining data comprising the content file to determine whether the content file includes a restricted data format, wherein the content file is free of a digital signature, transmitting the data file if data comprising the content file does not include the restricted data format, and blocking the file if data comprising the content file does include the restricted data format (col. 1, lines 36-40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine examining data comprising the content file to determine whether the content file includes a restricted data format, transmitting the data file if data comprising the content file does not include the restricted data format, and blocking the file if data comprising the content filed does include the restricted data format, as taught by Boyle et al., to the network infrastructure of Gupta et al. It would have been obvious for such modifications because examining the content file and transmitting based on the lack of the restricted data format or blocking based on the presence of the restricted data format prevents network congestion. By only allowing text and other small data files to transmit, the burden of transmitting video or audio is

eliminated. This is especially important when the receiving device can't handle the restricted data type (see col. 1, lines 38-40 of Boyle et al.).

The combination of Gupta et al. in view of Boyle et al. does not teach **using at least one router configured to log digital signatures related to the content file**. However, Gibbs et al. teaches **using at least one router configured to log digital signatures related to the content file** (fig. 4, ref. num 432 and col. 6, lines 17-26).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a router configured to log digital signatures related to the content file, as taught by Gibbs et al., to the network infrastructure of Gupta et al/Boyle et al. It would have been obvious for such modifications because the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network would keep track of the status information and other information about the creation and authentication of digital signatures (see col. 3, lines 63-66 of Gibbs et al.).

Regarding claims 18, and 19, the combination of Gupta et al. in view of Boyle et al./Gibbs et al. teaches the restricted data format is an MP3 data format, a MPEG video data format, and a Word document format (see col. 1, lines 36-40 of Boyle et al.).

Claims 3, 6, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gupta et al. (USPN '532) in view of Boyle et al. (USPN '636) and Bruck et al. (USPN '165), and further in view of Gibbs et al. (USPN '321).

Regarding claim 3, the combination of Gupta et al. in view of Boyle et al./Bruck et al. teaches all of the subject matter of claim 1, as discussed above. However, the combination of Gupta et al. in view of Boyle et al./Bruck et al. does not disclose the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network.

Gibbs et al. teaches the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network (fig. 4, ref. num 432 and col. 6, lines 17-26).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network, as taught by Gibbs et al., to the digital signature method of Gupta et al. in view of Boyle et al./Bruck et al. It would have been obvious for such modifications because the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network would keep track of the status

information and other information about the creation and authentication of digital signatures (see col. 3, lines 63-66 of Gibbs et al.).

Regarding claims 6 and 13, the combination of Gupta et al. in view of Boyle et al./Bruck et al. teaches all of the subject matter of claims 1 and 7, respectively, as discussed above. However, Gupta et al. in view of Boyle et al./Bruck et al. does not disclose the examining is performed by a plurality of cache engines within the distributed computer network.

Gibbs et al. teaches the examining is performed by a plurality of cache engines within the distributed computer network (fig. 4, ref. num 420 and col. 7, lines 13-28).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to use a plurality of cache engines to perform the examining within the distributed computer network, as taught by Gibbs et al., with the methods of Gupta et al. in view of Boyle et al./Bruck et al. It would have been obvious for such modifications because the use of a plurality of cache engines to perform examining within the distributed computer network would allow faster examining of data as it is passed over the distributed computer network (see col. 7, lines 15-25 of Gibbs et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100